2.0 NLETS NETWORK ACCESS

2.0 NLETS NETWORK ACCESS

2.1 INTRODUCTION

The purpose of Nlets, the International Public Safety Network, is to provide a network for law enforcement, criminal justice, and other agencies and organizations to exchange information. The nature of the Nlets mission and the sensitivity of the data require stringent controls to assure no abuses of the network occur. This section describes these policies.

2.1.1 NCIC POLICIES

Much commonality exists between the FBI's Criminal Justice Information System (CJIS) - National Crime Information Center (NCIC) mission and that of Nlets as it relates to the accessibility and sharing of criminal justice information. The CJIS Security Policy provides the minimum level of Information Technology (IT) security requirements determined acceptable for the transmission, processing, and storage of the nation's Criminal Justice Information Systems (CJIS) data.

Where applicable, Nlets has adopted and complied with the security requirements set forth in the CJIS Security Policy. Moreover, to ensure uniform application and implementation of security standards, the Nlets Security Policy will be managed and monitored in a like fashion.

2.2 NETWORK ACCESS

The Nlets network and subsequent data are protected by a complex set of inextricably interwoven software and hardware security features. In addition, the implementation of, and adherence to, strict membership requirements as well as on-going review and monitoring ensures the overall integrity of the system.

2.2.1 ACCESS APPROVAL

Network access application process:

1) Make formal written request for access in compliance with Nlets policies

2) Obtain Nlets Board approval – (requirement for requesting entity to become a member is evaluated on a case-by-case bases)

3) Once approved and designated as the Nlets System Agency (NSA) for the requesting entity, the controlling body of that entity must appoint an Nlets System Officer (NSO). Once appointed, the NSO is ultimately and finitely responsible for all transactions and activity generated from, or on behalf of, that entity.

4) The NSO must sign and execute all agreements and documents certifying the requesting entity is, and will remain, in compliance with all security standards, policies, procedures, and training requirements set forth by Nlets.

2.2.2 REQUIREMENTS OF THE NLETS SYSTEM AGENCY (NSA)

The NSA is the focal point for Nlets and is responsible for assuring only authorized persons and entities access Nlets through their interface. Exceptions are those agencies that are authorized to obtain criminal history information (CHRI) through PL99-169 "The Intelligence Authorization Act of Fiscal Year 1986", Title VIII, Section 910 (entitled "Access of Criminal History Records for National Security Purposes").

Section 1.4.1 of this guide illustrates the types of agencies authorized to access Nlets and any restrictions regarding the information they are authorized to obtain. An up-to-date list of agencies approved for access by the Nlets Board of Directors may be obtained through Nlets Administrative Office (623) 308-3500. The NSA must also assure information obtained via Nlets is used only for official authorized purposes.

Included in the definition of "authorized purposes" are:

- The review of message traffic for quality control.
- The usage of traffic for statistical analysis purposes.

The NSA must be manned 24 hours per day, seven days per week unless approved for less than this by the Nlets Board of Directors an agreement is signed by the NSAs to formalize these responsibilities.

2.2.3 AUTHENTICATION AND IDENTIFICATION

The state must assure that only authorized users will access Nlets. The state must provide these assurances on two levels:

- The creation and certification of all ORIs.
- The identification and authentication, at the individual level, of all persons that access the network.

This policy applies to all individuals that transmit information to Nlets through the NSA's interface to Nlets.

2.2.3.1 ORION VALIDATION, CREATION, AND CERTIFICATION

The objective of the ORION File is to assure that only authorized users are using the network and these users are using the network for authorized purposes. Once created, Nlets ensures that it is both accurate and complete.

Validation

Validation of sending ORIs must be accomplished on every transaction passed to Nlets.

Creation

Only NCIC approved ORIs, Nlets generic ORIs and Board approved ORIs may be entered on Nlets. For example, Indiana may not enter an Illinois ORI. Only terminals authorized by the NSA may add entries to ORION. The "add/cancel" authorization flag can be manipulated only by the NSA ORI. After initial creation, Nlets will print every ORI that is added to the file. They will be checked against NCIC's ORI file to determine whether it is on NCIC. If it is not, it must have been approved by the Board of Directors.

Once approved for access, Nlets controls daily access to the network through comparison to an Nlets-resident table of authorized ORIs called the ORI On-line Directory (ORION). The sender and destination ORIs are checked on every transmission sent through the network. Nlets also uses the ORI in conjunction with ORION to control the types of information sent through the network. It is therefore a critical piece of every transmission over the network.

Nlets divides ORIs into two types: criminal justice and non-criminal justice ORIs.

- The non-criminal justice agencies are further divided:
- Those that have an ORI assigned by the FBI
- Those that have an ORI assigned by Nlets.

When a criminal justice agency performs a service on behalf of a governmental non-criminal justice agency, each agency must have an ORI. In all transactions the ORI of the governmental non-criminal justice agency must be used. If the non-criminal justice agency does not have an ORI and is using Nlets for approved purposes, Nlets staff will assign an Nlets ORI. This is the “S” ORI.

If the non-criminal justice agency contracts with a private firm, there must be an agreement signed by a representative from the non-criminal justice agency, the private contractor and the Nlets representative. This agreement guarantees that the non-criminal justice agency will assure that Nlets policies and procedures are followed by the private contractor.

All law enforcement and criminal justice agencies in the United State and Canada are authorized to access Nlets.

There are many non-criminal justice agencies that are authorized to access Nlets. These fall into three groups as described below.

Generic Types of Agencies

Non-Criminal Justice Governmental Agencies with an FBI ORI

These agencies have been assigned an ORI by the FBI but are not criminal justice agencies.

Example: Department of Motor Vehicles (DMV) within the states.

Non-Criminal Justice Governmental Agencies with an Nlets ORI

These agencies have been assigned an ORI by Nlets but are not criminal justice agencies. These ORIs may be identified by an “s” in the 9th character.

Example: A child support enforcement agency within a state.

Private Not-for-Profit Organizations with an Nlets or NCIC ORI

These organizations may have an ORI assigned by the FBI or Nlets. Through their membership they provide a service to the law enforcement or criminal justice community. These Nlets ORIs may be identified by an “S” in the 9th character.

Example: An organization such as the National Insurance Crime Bureau (NICB).

Certification

It is the responsibility of the Nlets representative to ensure that all ORION entries owned by that user (state, federal, international or associate) have been certified as up to date and accurate at least every two years. These dates will coincide with NCIC's validation of their ORI file.

Every two years a printed listing or other form of storage media containing all ORIs will be mailed to each Nlets representative. The Nlets representative will certify that all records are valid, accurate and up to date. He or she will then sign a certification document attesting to the validity of each record owned by the member. Nlets staff will cause the certification date in each record to be updated to reflect the successful completion of the certification procedure. Users will have 90 days to certify their ORIs.

Following the 90 day certification period, Nlets will notify members who have not certified their ORI file that their ORIs will be deactivated in thirty days unless certified within that time period. A return receipt for the second notice will be requested. If after thirty days from the time the member has received the second notice, the ORIs still have not been certified, the ORIs will be deactivated.

2.2.3.2 AUTHENTICATION AND IDENTIFICATION

Authentication and identification may be accomplished by several methods including password systems, digitized signatures, smart cards, fingerprint verification or other biometric methods. Each user that accesses Nlets must be identified and authenticated using one of these methods. The state Nlets System Agency (NSA) must verify that this is being done and re-verify when ORI validation takes place.

If there are other methods that a state believes will provide the same or a greater level of identification and authentication, they may be submitted in writing to the Nlets administrative office for consideration. Nlets recognizes that local agencies may have the ability to access the FBI's Law Enforcement Online (LEO) or other networks through the existing Nlets Frame Relay network. This access however must go through and be controlled / screened by the NSA's system.

All Nlets members must have complied with the authentication and identification policies by July 2002. Members are expected and encouraged to implement this policy whenever upgrades are implemented within their state or local systems.

2.2.4 ENCRYPTION

All intelligence information or criminal history record information received from Nlets and passing through an unprotected domain that is not dedicated to criminal justice purposes shall be encrypted while in that domain. If intelligence or criminal history record information is received from Nlets and transmitted over wireless links, dial-up or Internet connections, it must be protected with encryption. All agencies that utilize an unprotected domain as a part of their connectivity to Nlets must comply with encryption requirements.

It is not the intent of this policy to dictate a specific encryption solution. A variety of hardware and software solutions are available, (i.e., session-based and Virtual Private Networks-VPNs). It is envisioned that the use of either private-key or public-key systems will be acceptable. Private-key systems shall be based on FIPS Publication 46-2, Data Encryption Standard (DES). DES is also defined in ANSI X3.92, ANSI X3.106, and FIPS Publication 81. The use of cryptographic techniques should employ at least a 56-bit key.

All Nlets members must have complied with this policy by July 10, 2002. Members are expected and encouraged to implement this policy whenever upgrades are implemented within their state or local systems.

2.2.5 FIREWALLS

Firewalls or devices offering equal protection shall be installed at those points in the network where electronic intrusion by unauthorized users is possible. Any federal, state, county, city or other network in which there is direct connectivity to both Nlets and the Internet must include a firewall type device to prohibit unauthorized traffic from traversing the Nlets network.

Application level firewalls should provide the capability to screen traffic at the application, network and transport layers, as well as the ability to authenticate end users with additional audit capability. The firewall configuration must have the following capabilities/components:

- The firewall selected must have a secure operating system that can protect its own internal code and files from intruder attack.
- The firewall, or a separate filter placed immediately outside the firewall, must intercept all packets and permit only authorized communications to pass.
- The firewall or gateway component must intercept traffic and authenticate users at the application level. This can be accomplished by implementing a proxy server for each type of application or by customizing client software to use a utility server such as SOCKS.
- The firewall configuration must include a component to provide domain name service. Domain name service isolates internal addresses from outside exposure.
- The firewall configuration must include a component to provide a secure mail handling capability that ensures that any e-mail exchange is authorized.

All Nlets members must have complied with this policy by July 10, 2002. Access to the Internet may not be added to an existing state, local or federal network without installing adequate firewall protection.

2.2.6 INTERNET ACCESS

This policy applies to your state if any agency that you provide Nlets access has a hard wire connection to an Internet Service Provider (ISP). Agencies that utilize Internet by dialing up through their PC do not create a significant threat and are exempt from these policies.

Those qualifying agencies must either:

A. Install a firewall between the system connected to Nlets and the Internet.

- The firewall selected should have a secure operating system that can protect its own internal code and files from intruder attack.
- No other non-security applications should be allowed on the firewall.
- The firewall must intercept all packets and permit only authorized communications to pass.
- Adequate authentication and packet screening controls must be present to reduce the chance of IP address spoofing.
- The firewall must have an application gateway component that intercepts traffic and authenticates users at the TCP/IP application level.
- Practice virus screening.
- The firewall is only a tool for security. States should have a plan in place on how to respond to security breaches and report all intrusions to the appropriate system administrator, such as the Nlets Executive Director. States are encouraged to keep the operating system changes current on their firewall.

OR

B. In the absence of a firewall, the Nlets representative must provide a description of safeguards that provide an acceptable level of security to protect Nlets and insure that Internet users cannot access Nlets users.

2.2.7 DIAL-UP ACCESS

Any routine access to the Nlets System through the Point of Entry (POE) over commercial switched circuits on a continuous or temporary basis is authorized provided that appropriate security measures are in place. There are a variety of security conventions that may be adopted including use of passwords, personal descriptors, biometrics, encryption, token devices, terminal authentication and message authentication. The ultimate decision regarding the adequacy of the security measure rests with the Nlets System Agency (NSA).

The NSA has the following responsibilities regarding to dial-up access:

- The NSA has authority to approve and operate dial-up access, providing the appropriate security measures are in place.
- The NSA is responsible for documenting the security measures in place and for the administration of the dial-up system. This includes user identity and agency association, and the level of access the user is authorized.
- The system will be able to identify and authenticate the dial-in user prior to the user gaining access to Nlets. The system must be capable of establishing a number, serial number, or other unique character string.

- All transactions and messages sent and received on the dial-up system must be logged. The system must be able to identify the transaction from the automated transaction log for all dial-up circuits. Automatic logging includes session initiation and termination messages, failed access attempts, and all forms of access violations such as attempts to access data beyond the level of authorized access.
- Access to the transaction log should be highly controlled. The transaction log should not be vulnerable to modification if the system is penetrated.

2.2.8 CONTROL AND DISTRIBUTION OF INFORMATION OVER NLETS

Each State, Federal, Associate and International member granted an interface to Nlets is responsible for providing access for their criminal justice agencies or other authorized agencies to all other criminal justice or other authorized agencies in the nation. With this responsibility, the member has the authority, and must exercise the authority, to insure that all users follow the Nlets policies relating to security of the information transmitted on the system.

One of the required Nlets safeguards is the requirement that all members include a plain English message identifying all non-criminal justice users that send "AM" messages over Nlets. The message states "MESSAGE INITIATED BY A NON-CRIMINAL JUSTICE AGENCY."

Nlets validates all ORIs that pass through the network. Users must certify that their file of ORIs is accurate and up to date on a biennial basis. This adds an additional level of security to the network.

2.2.9 SECONDARY DISSEMINATION

Information requested by an authorized agency may be provided to another agency provided that:

- The agency receiving the secondary dissemination is authorized by Nlets policies to directly access this information over Nlets.
- The information is current.

For example if a law enforcement agency requests a registration on a vehicle for criminal justice purposes, they may provide this information to a prosecutor since both agencies are authorized to request this information directly under current Nlets policies. Users should not disseminate stale or outdated information to a secondary recipient. A new inquiry should be made and the most recent record used.

2.2.10 CRIMINAL HISTORY INFORMATION ACCESS

Only agencies that have an FBI/NCIC assigned law enforcement or criminal justice ORI are authorized to request criminal history record information (CHRI) over Nlets. The members must assure that only these authorized agencies are able to use these ORIs in their requests that are sent to another agency through Nlets. Nlets will assure that all ORIs making requests for CHRI are duly authorized. The state must also assure that the requester indicates the purpose for which the request is being made. This is critical information because states differ as to the purposes which they, by statute or rule, can honor.

Below is a list of the allowable purposes along with the codes that must be included in all CHRI requests.

Purpose Codes for CHRI Requests

Code	Explanation
C	Must be used when the IQ, FQ, or AQ is for official duties in connection with the administration of criminal justice.
E	Must be used for employment and licensing.
J	Must be used when the IQ, FQ, or AQ involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control. Criminal justice employment has been separated from other criminal justice purposes due to the requirement of some state agencies.
F	Must be used by criminal justice agencies in all states for screening applications for firearms and related permits. This includes firearms dealers, firearms purchases, carriers of concealed weapons, explosive dealers and users, and lethal weapons dealers and users, but only when a Federal, state or local law/ordinance exists making the criminal justice agency responsible for the issuance of the licenses/permits.
D	Must be used by courts when hearing civil domestic violence or stalking cases. This purpose code shall not allow access to State sealed records.
S	Must be used by Defense Investigative Service and any other SCIA agencies authorized specifically by NLETS to access CHRI through the network using IQ, FQ, and AQ.
X	For use in conducting checks involving the emergency placement of children when unaccompanied by the immediate submission of fingerprints on the surrogate care provider(s).

2.2.11 USER AGREEMENT

Each member must sign a joint Nlets/Member Agreement that indicates that they will follow all Nlets rules, policies and procedures. Many states have also signed agreements with the local and county agencies to assure that all Nlets policies are being followed at the terminal level. A copy of the Nlets Users Agreement is included at the end of Section 1 of this guide.

2.2.12 NLETS PHYSICAL SECURITY

Concern for Nlets security involves the physical security of the facility and the assurances that appropriate background checks have been conducted on personnel operating the network.

2.2.12.1 NLETS COMPUTER CENTER PHYSICAL SECURITY

The Nlets Computer Center is located on the grounds of the Arizona Department of Public Safety. Restricted access to the Nlets Center will be maintained by the use of card readers or similar methods for assuring that only authorized personnel may gain entrance to the Center.

2.2.12.2 NLETS PERSONNEL SECURITY

The Arizona Department of Public Safety conducts a background investigation for all Nlets employees. Two sets of fingerprint cards are taken on each new employee hired by Nlets who will occupy space on the DPS premises. One set of fingerprint cards is retained in the DPS Human Resources section as part of a permanent record for all contract employees. The second set is forwarded to the FBI for a complete background review that includes a criminal history check and any outstanding wants or warrants.

2.3 GLOSSARY OF TERMS

Term	*Description*
Application Layer	Layer 7 of the Open Systems Interconnection (OSI) reference model. The layer closest to the user that provides service to application processes, such as e-mail and file transfer.
Authentication	The process of determining whether a requesting user has been authorized to perform the requested action (e.g., request criminal record information).
Biometric Methods	Historically, computer security has been based on two authentication methods: something you know (e.g., passwords) or something you have (e.g., smart cards, tokens). A third security method has emerged: something you are, otherwise known as biometrics. Biometrics can be used to authenticate a fingerprint, retina, hand, face, voice, or some other physical characteristic.
Criminal History Record Information	CHRI -Criminal History Record Information is arrest-based data and any derivation information from that record, i.e. descriptive data, FBI number, conviction status, sentencing data, incarceration, probation and parole information.
Nlets System Agency	The agency designated by the Nlets member that is responsible for ensuring all rules, policies, and procedures are followed by all users to which they provide access.
Digitized Signatures	A digital signature is a seal of confidence which enables the recipient of a message to authenticate the sender of a message and verify that the message was intact or not modified as it was sent. The digitally signed message must be done by the sender, so the recipient must request such a document.
Domain Name	All computers on the Internet have a unique number called an IP address. These IP addresses are neither intuitive nor easy to remember. An IP number like 234.12.34.212 is replaced with a simple alias called a domain name. A domain name is divided up into 3 sections. In the following (fictional) domain name: funny Kentucky.blue-grass.com ".com" is the top domain, "blue-grass" is the sub-domain and "funny Kentucky" is an extra bit that was attached later.
Domain Name Service (DNS)	A system used in the Internet for translating names of network nodes into addresses.

Term	*Description*
Firewalls	A firewall is a software program at the boundary of a network, which acts as gatekeeper between a company's internal network and the outside world. At a minimum, the firewall examines the location from which data enters the system or the location to which data are going, and then chooses, based on instructions, whether to allow the transfer of that information. In addition to gate keeping functions most firewalls monitor the use of a system and keep logs so the administrator knows if anyone is trying to break in. For example, if someone tries to log on to a system five times with the wrong password, the firewall's activity report will show that. Some firewalls E-mail or page the systems administrator when they detect suspicious activity. Other firewalls offer encryption options, which allow the user to scramble the information in files, making it unreadable. Various access policies and authentication levels can be set up as well logging of all users who traverse through firewalls.
Frame Relay	A packet-oriented network access protocol that provides for the establishment of connections and the transfer of data across these connections. Packet-oriented protocols provide a way to allocate bandwidth intelligently on an as-needed basis instead of through fixed channel allocation (the old dedicated circuits).
Identification	The process of determining if a request user is authorized to enter the system.
Intelligence Information	Information or files created that may assist law enforcement agencies in the apprehension and conviction of suspects in a variety of criminal activity. An example of intelligence information could include informant or surveillance information.
Internet	Term used to refer to the world's largest inter-network connecting thousands of networks worldwide.
LEO	Law Enforcement Online (LEO) is an Intranet service operated by the FBI and serving primarily law enforcement and criminal justice agencies.
Network Layer	Layer 3 of the OSI reference model. This layer provides connectivity and path connection between two end systems. The network layer is the layer at which routing occurs.
Permanent Virtual Circuit (PVC)	A virtual or logical circuit that is permanently established and set up between two network devices.
Proxy Server	An entity that in the interest of efficiency stands in for another entity.
Session-Based	Transmission control: Provides a reliable end-to-end connection service. The originating station negotiates communications parameters with receiving station and sets up a permanent communications session (a virtual circuit) until communication is complete and then tears down (terminates) the virtual circuit. This is a reliable transport mechanism since an acknowledgment is sent for every window of data.
Smart Cards	A smart card is a credit-card sized plastic card with an embedded computer chip. The chip can either be a microprocessor with internal memory or a memory chip with non-programmable logic. The chip connection is either via direct physical contact or remotely via a contactless electromagnetic interface.

Term	***Description***
SOCKS	SOCKS is a proxy protocol for client/server environments. SOCKS includes two primary components, the SOCKS server and the SOCKS client library. The SOCKS server implementation is at the application layer and the SOCKS client library is between the client's application and transport layers. Currently there are two versions of the SOCKS protocol, version 4 and version 5. The SOCKS version 4 protocol is often referred to as "SOCKS V4". Similarly the SOCKS version 5 is referred to as "SOCKS V5".
Transmit Information	The act of sending information over the Nlets Frame Relay network.
Transport Layer	Layer 4 of the OSI reference model. This layer is responsible for reliable network communication between end nodes. The Transport Layer provides mechanisms for the establishment, maintenance and termination of virtual circuits, transport, fault detection and recovery and information flow control.
Unprotected Domain	Any computer network or system that lacks the security features deemed necessary by its users to protect the integrity of its resources.
Virtual Private Network (VPN)	Virtual Private Network (VPN) is a seamless "private" network by making use of public routed network, such as the Internet or other commercially available network, in a private "tunnel" that simulates a point-to-point connection. A "tunnel" is a secure data path between the two endpoints, which is controlled by only the two end users. Tunnel security is achieved by EEA, i.e. Encapsulation, Encryption and Authentication.
Wireless Links	A wireless link is a communications medium between two points using RF (radio frequency) waves. The two devices are tuned to the same frequency using the same modulation technique. An example of wireless links is LAWN (Local Area Wireless Network) and mobile data systems.